MEB:ADW
F. #2019R01108

UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

IN THE MATTER OF THE SEARCH OF INFORMATION ASSOCIATED WITH APPLE ID ACCOUNT 8238769227 AND APPLE ID ACCOUNT 16782022072 THAT IS STORED AT PREMISES CONTROLLED BY APPLE, INC.	**TO BE FILED UNDER SEAL** **APPLICATION FOR A SEARCH WARRANT FOR INFORMATION IN POSSESSION OF A PROVIDER** Case No. 21-MJ-60

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Alex Turczak, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require Apple Inc. (hereinafter "Apple") to disclose to the government records and other information, including the contents of communications, associated with Apple ID account 8238769227 ("SUBJECT ACCOUNT #1") and Apple ID account 16782022072 ("SUBJECT ACCOUNT #2," and together with SUBJECT ACCOUNT #1, the "SUBJECT ACCOUNTS") that are stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA. The information to be disclosed by Apple and searched by the government is described in the following paragraphs and in Attachments A and B.

2. I am a Special Agent with the Federal Bureau of Investigation ("FBI") and have been since September 2017. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged

in enforcing the criminal laws and duly authorized by the Attorney General to request a search warrant. I have participated in numerous investigations of violations of federal offenses including wire fraud, bank fraud and money laundering. I have also received training on the uses and capabilities of cellular telephones and other electronic devices in connection with criminal activity.

3. The facts in this affidavit come from my personal observations, my training and experience and information obtained from other agents and witnesses. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

4. Based on the facts set forth in this affidavit, there is probable cause to believe that the SUBJECT ACCOUNTS will contain evidence of violations of 18 U.S.C. §§ 1343 (wire fraud), 1344 (bank fraud), 1349 (bank and wire fraud conspiracy) and 1956 (money laundering and money laundering conspiracy) (collectively, the "SUBJECT OFFENSES"). There is also probable cause to search the information described in Attachment A for evidence of this crime as further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is "a court of competent jurisdiction" as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is "a district court of the United States . . . that has jurisdiction over the offense being investigated." 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. As described in detail below, KENENTH UKHUEBOR and PATIENCE OSAGIE own and control several bank accounts that have received substantial sums of money

from the victims of certain fraud schemes. The first scheme involved false promises to individuals that they would be entitled to large foreign inheritances upon payment of certain advance fees and charges. The second scheme involved fraudsters using hacked or false email accounts to deceive companies into diverting payments into certain bank accounts. UKHUEBOR and OSAGIE controlled bank accounts that received proceeds from both of these fraud schemes. As described in this affidavit, UKHUEBOR and OSAGIE received in these accounts at least $8 million in fraudulent proceeds. In addition, UKHUEBOR and OSAGIE appear to have used the email address kenborpat@yahoo.com to not only register numerous bank accounts involved in their money laundering scheme, but also register SUBJECT ACCOUNT #1 with Apple. Separately, SUBJECT ACCOUNT #2 is associated with UKHUEBOR and OSAGIE's residential address, and both SUBJECT ACCOUNTS appear to be associated with certain electronic devices that were seized from that address. Based on those facts, there is probable cause to believe that records and other information, including the contents of communications, associated with the SUBJECT ACCOUNTS will provide evidence regarding KENNETH UKHUEBOR's and PATIENCE OSAGIE's involvement in the SUBJECT OFFENSES.

The Suspects, Kenbor Inc. and Related Bank Accounts

7. Based on information and belief, KENNETH UKHUEBOR and PATIENCE OSAGIE are individuals both residing in Queens, New York.

8. Kenbor Inc. is a business corporation registered in New York State. Based on New York State Division of Corporations records, Kenbor Inc. was first registered in March 2015 and lists PATIENCE OSAGIE as the person who should receive any legal process on behalf of the company. As described below, Kenbor Inc. appears to be either the business

operating name or the parent company of a clothing store operating as Kenbor Clothing. "Kenbor" appears to be a combination of "Kenneth" and "Ukhuebor."

9. On the business social networking website LinkedIn, a search for the name "Patience Osagie" yields several results. Only one of the results is for a user listed as residing in the New York area. The Patience Osagie residing in the New York area describes her work experience as being a boutique owner and fashion designer at Kenbor Inc. since January 2015. Notably, this account displays as a profile picture a heavyset adult male with a distinctive beard and wearing sunglasses. Based on my familiarity with the investigation to date, this appears to be KENNETH UKHUEBOR.

10. Through my investigation, I have identified two separate accounts on the social networking website Facebook, Inc. ("Facebook") that appear to belong to KENNETH UKHUEBOR. The username for one of the accounts is "Kenneth Ukhuebor," and the username for the other account is "Ken Kenbor." Both accounts display profile pictures and other photographs depicting the same heavyset adult male shown in the profile picture for the aforementioned Patience Osagie LinkedIn account. Based on records I have received from Facebook, I know that the "Ken Kenbor" account was registered with the kenborpat@yahoo.com email address.

11. PATIENCE OSAGIE appears to have a Facebook account that displays the name "Precious Ukhuebor." The "Precious Ukhuebor" Facebook account displays profile photos and other pictures of OSAGIE and lists the user as "married." On February 14, 2020, the Precious Ukhuebor Facebook account posted a photo of OSAGIE with KENNETH UKHUEBOR and included a Valentine's Day message. In addition, OSAGIE appears to have an account (username "ukhuebor_precious") on Instagram, a social networking site that allows users to post

pictures with captions. OSAGIE's Instagram page includes numerous photos of UKHUEBOR with accompanying descriptions that refer to him as her husband.

12. The URL for the Precious Ukhuebor Facebook account is www.facebook.com/patience.osagie.3958.

13. On the Precious Ukhuebor Facebook account, PATIENCE OSAGIE describes her employment as "Kenbor Clothing," using a clickable link that leads to a "Kenbor Clothing" Facebook page. The page describes the business as a "Women's Clothing Store" and includes a post from October 16, 2019 announcing a grand opening. The Kenbor Clothing Facebook page displays the following image as its profile picture.

14. On October 16, 2019, PATIENCE OSAGIE changed her Facebook profile picture to display the same Kenbor Clothing picture above. Also on October 16, 2019, both the Ken Kenbor and Precious Ukhuebor Facebook users posted links to the Kenbor Clothing Facebook page's grand opening announcement.

15. Records from Facebook reveal that both the Kenbor Clothing and the Ken Kenbor accounts were registered using the same phone number.

16. Based on the foregoing, I believe that KENNETH UKHUEBOR and PATIENCE OSAGIE are married to each other or romantically involved with one another, and that UKHUEBOR is affiliated with Kenbor Inc. through OSAGIE.

17. KENNETH UKHUEBOR and PATIENCE OSAGIE maintained at least five bank accounts to receive funds, and to launder those funds, related to the Advanced Fee Inheritance Scheme and the Business Email Compromise Scheme.

18. Bank records I have reviewed indicate that in or about April 2013, KENNETH UKHUEBOR opened the bank account XXXXXX4749 (the "4749 Account") in his own name at a federally-chartered bank, the deposits of which were insured by the Federal Deposit Insurance Corporation ("FDIC"), and which conducts business in New York and other states ("Bank #1"). Based on my investigation in this matter, I know that the kenborpat@yahoo.com email address is associated with the 4749 Account.

19. Bank records I have reviewed indicate that in or about April 2015, PATIENCE OSAGIE opened the bank account XXXXXXXXX8304 on behalf of Kenbor Inc. (the "8304 Account") at a federally-chartered bank, the deposits of which were insured by FDIC and which conducts business in New York and other states ("Bank #2"). Based on my investigation in this matter, I know that the kenborpat@yahoo.com email address is associated with the 8304 Account.

20. Bank records I have reviewed indicate that in or about January 2019, PATIENCE OSAGIE opened the bank account XXXXXX3436 on behalf of Kenbor Inc. (the "3436 Account") at Bank #1. Those same records show that OSAGIE provided the kenborpat@yahoo.com email address when opening the account.

21. Bank records I have reviewed indicate that in or about February 2019, KENNETH UKHUEBOR opened the bank account XXXXXX4690 on his own behalf (the "4690 Account") at another federally-chartered bank, the deposits of which were insured by the FDIC, and which conducts business in New York and other states ("Bank #3"). Based on my investigation in this matter, I know that the kenborpat@yahoo.com email address is associated with the 4690 Account.

22. Bank records I have reviewed indicate that in or about September 2019, PATIENCE OSAGIE opened bank account XXXXX8113 on behalf of Kenbor Inc. (the "8113 Account"), which was maintained at Bank #3. Those same records show that OSAGIE provided the kenborpat@yahoo.com email address when opening the account.

The Advanced Fee Inheritance Scheme

23. Based upon my training and experience, I am familiar with fraud schemes referred to as "advanced fee" schemes. A typical advanced fee inheritance scheme often involve fraudsters who target elderly victims by pretending to be the representatives of a foreign estate in which the victim has purportedly been named as a beneficiary of the estate and is entitled to a large sum of money. Such schemes sometimes involve promises by fraudsters that the victim will receive a large payment upon the victim's payment to the fraudsters of purported taxes, fees or other invented charges.

24. As part of the government's investigation, I interviewed an individual victim located in New York ("Victim #1") who sent $53,400 to Kenbor Inc. pursuant to the Advanced

Fee Inheritance Scheme.[1] I also interviewed a personal assistant to Victim #1 (the "Assistant"), who provided me with copies of correspondence, faxes, and other documents relating to communications between Victim #1 and fraudsters. According to documents provided by the Assistant, a woman using the name "Catalina Moreno" (who held herself out as being a manager at a bank located in Spain) sent a letter to Victim #1 in November 2018, claiming that Victim #1 was entitled to a $26.7 million inheritance as long as Victim #1 first paid certain fees and charges. Victim #1 and Moreno then exchanged multiple messages via fax, with Moreno using a Spanish fax number. On or about December 18, 2018, Moreno sent Victim #1 a fax instructing him to write a check for $53,400 to Kenbor Inc. in connection with her claim that the payment to Kenbor Inc. would facilitate the release of millions of dollars in inheritance proceeds. That same day, Victim #1 wrote a check for $53,400 to Kenbor Inc. Later that day, an unknown individual deposited the $53,400 check into the 8304 Account, which, as described earlier, PATIENCE OSAGIE opened on behalf of Kenbor Inc. Victim #1 later informed me that he did not recognize the names of KENNETH UKHUEBOR or Kenbor Inc. and did not recall writing any checks to either UKHUEBOR or the company. Victim #1 never received any money or proceeds from Moreno or any other person or entity in connection with the purported inheritance

25. I have also interviewed a second victim of the Advanced Fee Inheritance Scheme, an individual victim residing in Washington ("Victim #2"). According to Victim #2, in or about March 2019, he received a call from an individual using the name "Arne Zeidler," who held

[1] Victim #1 died in February 2020.

himself out as a London-based lawyer.[2] Zeidler purportedly informed Victim #2 that he was entitled to a $10.5 million inheritance held at a United Kingdom bank called Yorkshire Bank, contingent on Victim #2 first paying certain fees and charges. On or about July 17, 2019, Zeidler sent Victim #2 an email, instructing him to wire funds to the 4690 Account in connection with false promises that the payment would facilitate the release of millions of dollars in inheritance proceeds. As described above, KENNETH UKHUEBOR had previously opened the 4690 Account in his own name. On or about July 18, 2019, Victim #2 wired $43,000 to the 4690 Account. Victim #2 never received any money or proceeds from Zeidler or any other person or entity in connection with the purported inheritance.

The Business Email Compromise Scheme

26. Based upon my training and experience, I am familiar with fraud schemes referred to as "business email compromise" schemes. A business email compromise ("BEC") scheme often involves a computer hacker gaining unauthorized access to a business email account via software, malware or social engineering, blocking or redirecting communications to and/or from the email account, and then using the compromised email account or a separate fraudulent email account (sometimes called a "spoofed" email account)[3] to communicate with

---

[2] Arne Zeidler appears to be an actual attorney based in London and founder of an international law practice called Zeidler Legal Services. The fraudster who communicated with Victim #2 appears to have impersonated the real Zeidler by creating and using the email address "azeidler@zeidlerlegalservice.com," whereas the real Zeidler's email address is "azeidler@zeidlerlegalservices.com."

[3] One way of spoofing an email address is to create an account at a fraudulent domain, where the domain name is altered to appear identical to a real company domain but where it is misspelled by a letter or character. For example, a BEC fraudster might spoof the email address

unsuspecting personnel from a victim company and trick them into making an unauthorized wire transfer. The fraudster directs the personnel to transmit company funds to the bank account of a third party (sometimes referred to as a "money mule"), which is often a bank account owned, controlled and/or used by individuals involved in the scheme. The money may then be laundered by transferring it through numerous bank accounts or by quickly withdrawing it as cash, by check or by cashier's check.

27. A New Jersey-based sign design, manufacturing and installation company that does business throughout the United States ("Company #1"), is one of the victims of the BEC scheme under investigation. Company #1 reported to the government that unidentified persons had gained access to its corporate email account and proceeded to send unauthorized emails to numerous corporate clients, inducing those clients into diverting wire payments to bank accounts controlled by fraudsters. For example, between June 2019 and July 2019, one client of Company #1 wired almost $400,000 to the 4749 Account at the direction of a fraudster sending an unauthorized email that purported to be from Company #1. As described earlier, KENNETH UKHUEBOR opened the 4749 Account in his own name in April 2013.

28. Another victim of the BEC scheme was a packaging company based in Georgia ("Company #2"). On or about May 8, 2019, Company #2 received two emails from a "spoofed" email account purporting to come from a vendor company. At the direction of the emails sent

---

of "John" at "ACME, Inc." (john@acmecompany.com) by creating similar email accounts at a fraudulent domain (e.g., john@acmecornpany.com, replacing the "m" in "company" with the letters "rn," or john@acmecompanies.com). Also, BEC fraudsters sometimes create a fraudulent email account at a legitimate email provider (e.g., john_acmecompany@gmail.com).

from the spoofed account, Company #2 redirected approximately $72,000 in payments to the 3436 Account. As described earlier, PATIENCE OSAGIE opened the 3436 Account in January 2019, in the name of Kenbor Inc.[4]

29. A publicly traded pharmaceutical company based in New Jersey and with offices in New York was a victim of the Business Email Compromise Scheme ("Company #3"). A pharmaceutical company based in New York ("Company #4") is a vendor for Company #3. As part of this investigation, I have interviewed representatives of Company #3 and received emails and other documents from them. According to those interviews and materials, in or about and between March 2020 and April 2020, Company #3 exchanged emails with an unknown fraudster that had gained unauthorized access to and was using the e-mail address of an employee of Company #4. On or about April 7, 2020, the person who had gained unauthorized access to the Company #4 account emailed a purportedly voided check to Company #3 in connection with requests to send future payments to the 8113 Account. As described earlier, PATIENCE OSAGIE opened the 8113 Account in September 2019 on behalf of Kenbor Inc. In or about April 2020 and May 2020, Company #3 wired more than $8,000,000 to the 8113 Account. Company #3 subsequently discovered the fraud and ceased making payments to the 8113 Account.

The Suspects' Money Laundering

30. After receiving proceeds of the advance fee inheritance and business email compromise schemes described above into bank accounts controlled by them, KENNETH

[4] Company #2 was able to reverse the transactions. As a result, neither PATIENCE OSAGIE nor anyone else with control over the 3436 Account was able to obtain the money.

UKHEUBOR and PATIENCE OSAGIE, together with others, withdrew cash, purchased checks, sent wire transfers, wrote checks, charged debit cards and used other methods of disposing of the proceeds to conceal and disguise the nature, location, source, ownership and control of the proceeds.

31. As described in paragraph 24, Victim #1 wrote a check for $53,400 to Kenbor Inc. on or about December 18, 2018, and an unknown individual deposited the check into the 8304 Account on the same day. On or about December 19, 2018, an unknown individual withdrew $30,000 in cash from the 8304 Account. And on or about December 20, 2018, an unknown individual withdrew $15,000 in cash from the 8304 Account.

32. As described in paragraph 25, Victim #2 wired $43,000 to the 4690 Account on or about July 18, 2019. On or about July 19, 2019, an unknown individual withdrew $8,500 in cash from the 4690 Account. On or about July 22, 2019, an unknown individual withdrew $29,980 in cash from the 4690 Account. And on or about July 24, 2019, an unknown individual withdrew $4,000 in cash from the 4690 Account and wired $700 to another bank account.

33. As described in paragraph 27, Company #1 wired almost $400,000 to the 4749 Account between June 2019 and July 2019. During that same period of time, bank surveillance camera footage shows that KENNETH UKHUEBOR withdrew large amounts of cash and wrote checks from the 4749 Account at multiple TD Bank locations. UKHUEBOR's pattern of withdrawals and checks appeared to closely match the timing and amounts of the wires from Company #1. For example, Company #1 wired $12,455.66 to the 4749 Account on June 14, 2019, and on June 17, 2020, UKHUEBOR debited $12,455 to the 4749 Account.

34. As described in paragraph 29, Company #3 wired more than $8,000,000 to the 8113 Account between April 2020 and May 2020. During that same period of time, a member or

members of the conspiracy withdrew cash from, wrote checks out of and charged debit cards to the 8113 Account in amounts totaling more than $1,000,000. More than $900,000 of the proceeds successfully drawn on the 8113 Account during this period were written out as checks. The signatures on all of those checks appear to be similar and consistent with the same signature of PATIENCE OSAGIE used to open the 8113 Account.

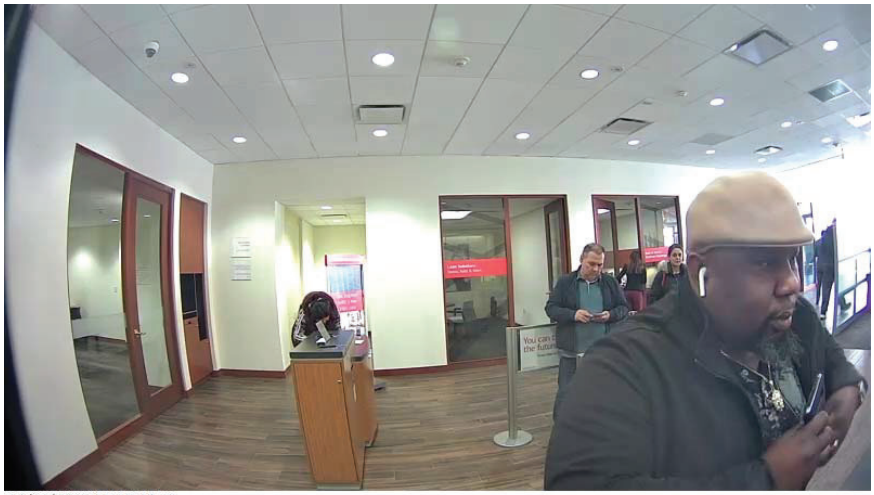
Additional Suspicious Bank Activity

35. As described below, KENNETH UKHUEBOR and PATIENCE OSAGIE appear to have also used one or more bank accounts held under a false name to perform large cash transactions in a manner that is consistent with the above-described pattern of money laundering

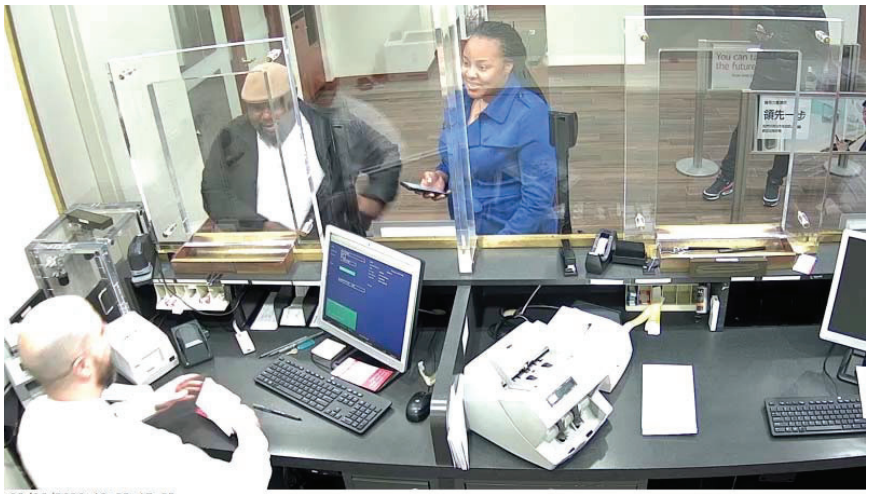
36. Records received from Bank #1, Bank #2 and several other banks show that an individual using the name "Alex Osato" currently maintains accounts with each of those banks. "Alex Osato" opened account number XXXXXX8586 (the "8586 Account") with Bank #1 using a Nigerian passport that appears to be fraudulent. "Alex Osato" also provided 2811 Avenue U in Brooklyn, New York 11229 as an address when opening the 8586 Account. This is the same address listed for Kenbor Clothing on its Facebook page and several online business listings.

37. "Alex Osato's" account with Bank #2 is assigned number XXXXXXXX3717 (the "3717 Account"). Bank records show that KENNETH UKHUEBOR and PATIENCE OSAGIE made withdrawals and deposits from the 3717 Account between February and April 2020. For example, the following surveillance camera image shows that UKHUEBOR made a $5,000 cash withdrawal from the 3717 Account on February 4, 2020:

38. The following surveillance camera image shows that KENNETH UKHUEBOR withdrew $4,000 in cash from the 3717 Account on March 4, 2020:



39. The following surveillance camera image shows that KENNETH UKHUEBOR and PATIENCE OSAGIE withdrew $9,000 in cash from the 3717 Account on March 6, 2020:



40. The following surveillance camera image shows that KENNETH UKHUEBOR withdrew $9,000 in cash from the 3717 Account on April 24, 2020:

The Arrests of KENNETH UKHUEBOR and PATIENCE OSAGIE

41. On December 3, 2020, the Honorable Sanket J. Bulsara, United States Magistrate Judge for the Eastern District of New York, issued warrants to arrest KENNETH UKHEUBOR and PATIENCE OSAGIE and to search their shared residential premises based on a supporting

complaint and affidavit sworn to by me. See Case No. 20-MJ-1155. The complaint charged UKHUEBOR and OSAGIE with money laundering conspiracy, in violation of Title 18, United States Code, Section 1956(a)(1)(B)(i).

42. The premises that was the subject of the above-mentioned search warrant was the second floor residential unit of 62-31 136th Street in Queens, New York (the "62-31 136th Street Address"). The 62-31 136th Street Address was the address provided by PATIENCE OSAGIE when she opened the 8304 Account and the 8113 Account and is also where she receives bank statements for those accounts.

43. On December 4, 2020, law enforcement arrested KENNETH UKHUEBOR and PATIENCE OSAGIE at the 62-31 136th Street Address. There were no other residents at the premises at the time of the arrest and subsequent search. Later on the same day, both UKHEUBOR and OSAGIE had their initial appearances before Judge Bulsara. Each of them was released on an unsecured $300,000 bond.

44. Based on the search of the 62-31 136th Street Address, agents recovered several electronic devices, including one Apple iPhone and one Apple iPad.

The SUBJECT ACCOUNTS

45. As described above, PATIENCE OSAGIE opened the 8304 Account, the 3436 Account, and the 8113 Account, and KENNETH UKHUEBOR opened the 4749 Account and the 4690 Account, all of which OSAGIE and UKHUEBOR appear to have used to receive and launder the proceeds of fraud schemes. OSAGIE provided the kenborpat@yahoo.com email address when she opened the 3436 Account and 8113 Account, and the investigation has separately shown that the kenborpat@yahoo.com email address is also associated with the 8304 Account, the 4749 Account and the 4690 Account. In addition, I know from my investigation

that OSAGIE and UKHUEBOR have each opened several other bank accounts, using the kenborpat@yahoo.com email address, that later received proceeds of the Advanced Fee Inheritance Scheme and the Business Email Compromise Scheme. Separately, the "Ken Kenbor" Facebook account is registered with the kenborpat@yahoo.com email address. These facts strongly suggest that UKHUEBOR and OSAGIE jointly use the kenborpat@yahoo.com email address, including in relation to their criminal activities.

46. Based on records I received from Apple on or about December 8, 2020, I know that PATIENCE OSAGIE registered SUBJECT ACCOUNT #1 using the kenborpat@yahoo.com address, and I believe that she registered it to access Apple-related services on an iPhone or other Apple devices. Those records also show that SUBJECT ACCOUNT #1 was first registered in February 2015, that the account was active as of December 2020, and that OSAGIE has configured SUBJECT ACCOUNT #1 to allow the following features to sync with Apple's iCloud service: (1) iCloud Backups; (2) bookmarks; (3) calendars; (4) photos; (5) iCloud Drive; (6) mail; and (7) notes.

47. In addition, Apple records show that PATIENCE OSAGIE registered SUBJECT ACCOUNT #2 using the email address osagie61291@yahoo.com, which I likewise believe was for the purpose of accessing Apple-related services on an iPhone or other Apple devices. Those records also show that SUBJECT ACCOUNT #2 was first registered in August 2019, that she provided the 62-31 136th Street Address as her address of record, that the account was active as of November 2020, and that OSAGIE has configured SUBJECT ACCOUNT #2 to allow the following features to sync with Apple's iCloud service: (1) iCloud Backups; (2) bookmarks; (3) calendars; (4) photos; (5) contacts; (6) iCloud Drive; (7) notes; and (8) Safari browsing history.

48. The Apple records indicate that in addition to storing information on Apple's servers via the services described above, both of the SUBJECT ACCOUNTS are regularly in contact with Apple's servers. For example, the Apple iCloud logs show that on November 25, 2020 and November 30, 2020, SUBJECT ACCOUNT #1 and SUBJECT ACCOUNT #2 each respectively conducted a "backup" from Apple devices, which, based on my training and experience, I believe is consistent with storing information from a user's Apple device to his or her iCloud account. Apple records also indicate that SUBJECT ACCOUNT #1 is associated with an Apple iPad and SUBJECT ACCOUNT #2 is associated with an Apple iPhone. As explained earlier, law enforcement seized one Apple iPad and one Apple iPhone from the 62-31 136th Street Address on December 4, 2020.

49. Furthermore, account activity on the SUBJECT ACCOUNTS has not only been recent, but also frequent. For instance, Apple records show that between November 8, 2020 and November 30, 2020, each of the SUBJECT ACCOUNTS accessed "iCloudDrive" and Apple's data backup functions hundreds of times.[5]

50. On or about November 25, 2020, law enforcement submitted a request to Apple to preserve all records and information associated with the SUBJECT ACCOUNTS.

51. Based on my training and experience, I know that individuals who engage in wire fraud, bank fraud and money laundering activities commonly use phones, computers, or other electronic devices to access websites used for illegal activity, to communicate with victims and

[5] Apple retains iCloud log histories for 30 days. Accordingly, the documents that I received from Apple on approximately December 8, 2020 did not reflect log histories from before November 8, 2020.

co-conspirators online, and to store records relating to transactions conducted as part of their illegal activities. As a result, such individuals often store data on their electronic devices related to their illegal activity, which can include logs of online chats with co-conspirators, electronic communications with victims, contact information of co-conspirators, and identifiers for instant messaging and social media accounts, as well as electronic records of financial transactions. In addition, to the extent such electronic devices are registered and back up data to Apple iCloud accounts, data relating to their illegal activities may be likewise stored on Apple servers.

52. In this particular case, there is probable cause to believe that KENNETH UKHUEBOR and PATIENCE OSAGIE used electronic devices to engage in wire fraud, bank fraud and money laundering. As the facts described above show, UKHUEBOR and OSAGIE controlled several bank accounts that received the proceeds of fraud schemes. Each time an account received fraudulent proceeds, UKHUEBOR and/or OSAGIE appeared to have withdrawn cash, debited funds or written checks from the relevant accounts in amounts that closely approximated the amounts of the fraudulent proceeds. Accordingly, I believe UKHUEBOR and OSAGIE actively monitored activity on their accounts using online banking services so that they could withdraw money as soon as possible after every fraudulent deposit or wire.

53. In addition, there is probable cause to believe that KENNETH UKHUEBOR and PATIENCE OSAGIE used electronic devices to communicate with co-conspirators in furtherance of the above-described schemes. Based on my training and experience in similar investigations, I know that UKHUEBOR's and OSAGIE's conduct is consistent with them acting as "money mules"—i.e., individuals who receive the proceeds of fraud committed by others and agree to transfer that money to others in return for being allowed to retain a share of

the proceeds. To do that, money mules necessarily need to communicate with co-conspirators so that they can share information regarding where victims are to send proceeds and where the money mules are to subsequently send the proceeds. In such schemes, money mules and co-conspirators usually communicate through electronic means such as email, text messages, social media platforms or other electronic written communication platforms because those are convenient means of sharing detailed information such as bank account information.

54. Because SUBJECT ACCOUNT #1 has been active for more than five years, is associated with kenborpat@yahoo.com (an email address that KENNETH UKHUEBOR and PATIENCE OSAGIE have used frequently in connection with their fraud and money laundering activities and at least one social media account), and appears to have been regularly used by either UKHUEBOR and/or OSAGIE since then in connection with at least one personal electronic device (i.e., the Apple iPad seized from the 62-31 136th Street Address on December 4, 2020), it is likely that SUBJECT ACCOUNT #1 is regularly used by either UKHUEBOR and/or OSAGIE in connection with their day-to-day online activities and communications.

55. Because SUBJECT ACCOUNT #2 was first activated in August 2019 (falling within the same time period that the apparent fraud and money laundering described above occurred), appears to have been regularly used by either KENNETH UKHUEBOR and/or PATIENCE OSAGIE since then in connection with at least one personal electronic device (i.e., the Apple iPhone seized from the 62-31 136th Street Address on December 4, 2020), and was registered to the 62-31 136th Street Address where both individuals were arrested, it is likely that SUBJECT ACCOUNT #2 is regularly used by either UKHUEBOR and/or OSAGIE in connection with their day-to-day online activities and communications.

56. Based on the foregoing facts, there is probable cause to believe that the records and other information, including the contents of communications, associated with SUBJECT ACCOUNT #1 and SUBJECT ACCOUNT #2 will provide evidence of the SUBJECT OFFENSES.

INFORMATION REGARDING APPLE ID AND ICLOUD[6]

57. Apple is a United States company that produces the iPhone, iPad, and iPod Touch, all of which use the iOS operating system, and desktop and laptop computers based on the Mac OS operating system.

58. Apple provides a variety of services that can be accessed from Apple devices or, in some cases, other devices via web browsers or mobile and desktop applications ("apps"). As described in further detail below, the services include email, instant messaging, and file storage:

a. Apple provides email service to its users through email addresses at the domain names mac.com, me.com, and icloud.com.

b. iMessage and FaceTime allow users of Apple devices to communicate in real-time. iMessage enables users of Apple devices to exchange instant messages ("iMessages") containing text, photos, videos, locations, and contacts, while FaceTime enables those users to conduct video calls.

---

[6] The information in this section is based on information published by Apple on its website, including, but not limited to, the following document and webpages: "U.S. Law Enforcement Legal Process Guidelines," available at http://images.apple.com/privacy/docs/legal-process-guidelines-us.pdf; "Create and start using an Apple ID," available at https://support.apple.com/en-us/HT203993; "iCloud," available at http://www.apple.com/icloud/; "What does iCloud back up?," available at https://support.apple.com/kb/PH12519; "iOS Security," available at https://www.apple.com/business/docs/iOS_Security_Guide.pdf, and "iCloud: How Can I Use iCloud?," available at https://support.apple.com/kb/PH26502.

c. iCloud is a file hosting, storage, and sharing service provided by Apple. iCloud can be utilized through numerous iCloud-connected services, and can also be used to store iOS device backups and data associated with third-party apps.

d. iCloud-connected services allow users to create, store, access, share, and synchronize data on Apple devices or via icloud.com on any Internet-connected device. For example, iCloud Mail enables a user to access Apple-provided email accounts on multiple Apple devices and on icloud.com. iCloud Photo Library and My Photo Stream can be used to store and manage images and videos taken from Apple devices, and iCloud Photo Sharing allows the user to share those images and videos with other Apple subscribers. iCloud Drive can be used to store presentations, spreadsheets, and other documents. iCloud Tabs and bookmarks enable iCloud to be used to synchronize bookmarks and webpages opened in the Safari web browsers on all of the user's Apple devices. iWork Apps, a suite of productivity apps (Pages, Numbers, Keynote, and Notes), enables iCloud to be used to create, store, and share documents, spreadsheets, and presentations. iCloud Keychain enables a user to keep website username and passwords, credit card information, and Wi-Fi network information synchronized across multiple Apple devices.

e. Game Center, Apple's social gaming network, allows users of Apple devices to play and share games with each other.

f. Find My iPhone allows owners of Apple devices to remotely identify and track the location of, display a message on, and wipe the contents of those devices. Find My Friends allows owners of Apple devices to share locations.

g. Location Services allows apps and websites to use information from cellular, Wi-Fi, Global Positioning System ("GPS") networks, and Bluetooth, to determine a user's approximate location.

h. App Store and iTunes Store are used to purchase and download digital content. iOS apps can be purchased and downloaded through App Store on iOS devices, or through iTunes Store on desktop and laptop computers running either Microsoft Windows or Mac OS. Additional digital content, including music, movies, and television shows, can be purchased through iTunes Store on iOS devices and on desktop and laptop computers running either Microsoft Windows or Mac OS.

59. Apple services are accessed through the use of an "Apple ID," an account created during the setup of an Apple device or through the iTunes or iCloud services. A single Apple ID can be linked to multiple Apple services and devices, serving as a central authentication and syncing mechanism.

60. An Apple ID takes the form of the full email address submitted by the user to create the account; it can later be changed. Users can submit an Apple-provided email address (often ending in @icloud.com, @me.com, or @mac.com) or an email address associated with a third-party email provider (such as Gmail, Yahoo, or Hotmail). The Apple ID can be used to access most Apple services (including iCloud, iMessage, and FaceTime) only after the user accesses and responds to a "verification email" sent by Apple to that "primary" email address. Additional email addresses ("alternate," "rescue," and "notification" email addresses) can also be associated with an Apple ID by the user.

61. Apple captures information associated with the creation and use of an Apple ID. During the creation of an Apple ID, the user must provide basic personal information including

the user's full name, physical address, and telephone numbers. The user may also provide means of payment for products offered by Apple. The subscriber information and password associated with an Apple ID can be changed by the user through the "My Apple ID" and "iForgot" pages on Apple's website. In addition, Apple captures the date on which the account was created, the length of service, records of log-in times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to and utilize the account, the Internet Protocol address ("IP address") used to register and access the account, and other log files that reflect usage of the account.

62. Additional information is captured by Apple in connection with the use of an Apple ID to access certain services. For example, Apple maintains connection logs with IP addresses that reflect a user's sign-on activity for Apple services such as iTunes Store and App Store, iCloud, Game Center, and the My Apple ID and iForgot pages on Apple's website. Apple also maintains records reflecting a user's app purchases from App Store and iTunes Store, "call invitation logs" for FaceTime calls, "query logs" for iMessage, and "mail logs" for activity over an Apple-provided email account. Records relating to the use of the Find My iPhone service, including connection logs and requests to remotely lock or erase a device, are also maintained by Apple.

63. Apple also maintains information about the devices associated with an Apple ID. When a user activates or upgrades an iOS device, Apple captures and retains the user's IP address and identifiers such as the Integrated Circuit Card ID number ("ICCID"), which is the serial number of the device's SIM card. Similarly, the telephone number of a user's iPhone is linked to an Apple ID when the user signs in to FaceTime or iMessage. Apple also may maintain records of other device identifiers, including the Media Access Control address ("MAC

address"), the unique device identifier ("UDID"), and the serial number. In addition, information about a user's computer is captured when iTunes is used on that computer to play content associated with an Apple ID, and information about a user's web browser may be captured when used to access services through icloud.com and apple.com. Apple also retains records related to communications between users and Apple customer service, including communications regarding a particular Apple device or service, and the repair history for a device.

64. Apple provides users with five gigabytes of free electronic space on iCloud, and users can purchase additional storage space. That storage space, located on servers controlled by Apple, may contain data associated with the use of iCloud-connected services, including: email (iCloud Mail); images and videos (iCloud Photo Library, My Photo Stream, and iCloud Photo Sharing); documents, spreadsheets, presentations, and other files (iWork and iCloud Drive); and web browser settings and Wi-Fi network information (iCloud Tabs and iCloud Keychain). iCloud can also be used to store iOS device backups, which can contain a user's photos and videos, iMessages, Short Message Service ("SMS") and Multimedia Messaging Service ("MMS") messages, voicemail messages, call history, contacts, calendar events, reminders, notes, app data and settings, Apple Watch backups, and other data. Records and data associated with third-party apps may also be stored on iCloud; for example, the iOS app for WhatsApp, an instant messaging service, can be configured to regularly back up a user's instant messages on iCloud Drive. Some of this data is stored on Apple's servers in an encrypted form but can nonetheless be decrypted by Apple.

65. In my training and experience, evidence of who was using an Apple ID and from where, and evidence related to criminal activity of the kind described above, may be found in the

files and records described above. This evidence may establish the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or, alternatively, to exclude the innocent from further suspicion.

66. For example, the stored communications and files connected to an Apple ID may provide direct evidence of the SUBJECT OFFENSES. Based on my training and experience, instant messages, emails, voicemails, photos, videos, and documents are often created and used in furtherance of criminal activity, including to communicate and facilitate the SUBJECT OFFENSES.

67. In addition, the user's account activity, logs, stored electronic communications, and other data retained by Apple can indicate who has used or controlled the account. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. For example, subscriber information, email and messaging logs, documents, and photos and videos (and the data associated with the foregoing, such as geo-location, date and time) may be evidence of who used or controlled the account at a relevant time. As an example, because every device has unique hardware and software identifiers, and because every device that connects to the Internet must use an IP address, IP address and device identifier information can help to identify which computers or other devices were used to access the account. Such information also allows investigators to understand the geographic and chronological context of access, use, and events relating to the crime under investigation.

68. Account activity may also provide relevant insight into the account owner's state of mind as it relates to the offenses under investigation. For example, information on the account may indicate the owner's motive and intent to commit a crime (e.g., information indicating a

plan to commit a crime), or consciousness of guilt (e.g., deleting account information in an effort to conceal evidence from law enforcement).

69. Other information connected to an Apple ID may lead to the discovery of additional evidence. For example, the identification of apps downloaded from App Store and iTunes Store may reveal services used in furtherance of the crimes under investigation or services used to communicate with co-conspirators. In addition, emails, instant messages, Internet activity, documents, and contact and calendar information can lead to the identification of co-conspirators and instrumentalities of the crime(s) under investigation.

70. Therefore, Apple's servers are likely to contain stored electronic communications and information concerning subscribers and their use of Apple's services. In my training and experience, such information may constitute evidence of the SUBJECT OFFENSES, including information that can be used to identify the account's user or users.

INFORMATION TO BE SEARCHED AND THINGS TO BE SEIZED

71. I anticipate executing this warrant under the Electronic Communications Privacy Act, in particular 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A), by using the warrant to require Apple to disclose to the government copies of the records and other information (including the content of communications and stored data) particularly described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.

CONCLUSION

72. Based on the forgoing, I request that the Court issue the proposed search warrant, pursuant to 18 U.S.C. § 2703(c) and Federal Rule of Criminal Procedure 41.

73. Because the warrant will be served on Apple, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

74. Pursuant to 18 U.S.C. § 2703(g), the presence of a law enforcement officer is not required for the service or execution of this warrant.

REQUEST FOR SEALING AND NON-DISCLOSURE

75. I further request that the Court order that all papers in support of this application, including the affidavit and search warrant, be sealed until further order of the Court. These documents discuss an ongoing criminal investigation, the scope of which is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may give targets an opportunity to destroy or tamper with evidence, change patterns of behavior or otherwise seriously jeopardize the investigation. Some of the evidence in this investigation involves communications that can be transferred to alternate platforms (including encrypted platforms and platforms beyond the jurisdictional reach of U.S. legal process). If alerted to the existence of the warrant, there is reason to believe that the targets and subjects under investigation will destroy that evidence and change their patterns of behavior.

76. Pursuant to 18 U.S.C. § 2705(b) and for the reasons stated above, it is further requested that the Court issue an Order commanding Apple not to notify any person (including subscribers or customers of the accounts listed in the attached warrant) of the existence of the

attached warrant for the period of one year from the date of the Order, except that Apple may disclose the warrant to its respective attorney for the purpose of receiving legal advice.

Respectfully submitted,

Alex Turczak
Special Agent
Federal Bureau of Investigation

Subscribed and sworn to before me by telephone on January 19, 2021

THE HONORABLE RAMON E. REYES, JR.
UNITED STATES MAGISTRATE JUDGE
EASTERN DISTRICT OF NEW YORK

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with the Apple ID accounts associated with account number 8238769227 and account number 16782022072 (the "SUBJECT ACCOUNTS") that is stored at premises owned, maintained, controlled, or operated by Apple, a company headquartered at 1 Infinite Loop, Cupertino, CA.

ATTACHMENT B

Particular Things to Be Seized

I. Information to Be Disclosed by Apple

To the extent that the information described in Attachment A is within the possession, custody, or control of Apple, regardless of whether such information is located within or outside of the United States, including any messages, records, files, logs, or information that have been deleted but are still available to Apple, or have been preserved pursuant to a request made under 18 U.S.C. § 2703(f, Apple is required to disclose the following information to the government, in unencrypted form whenever available, for each account or identifier listed in Attachment A:

a. All records or other information regarding the identification of each SUBJECT ACCOUNT, to include full name, physical address, telephone numbers, email addresses (including primary, alternate, rescue, and notification email addresses, and verification information for each email address, the date on which any SUBJECT ACCOUNT was created, the length of service, the IP address used to register any SUBJECT ACCOUNT, account status, associated devices, methods of connecting, and means and source of payment (including any credit or bank account numbers;

b. All records or other information regarding the devices associated with, or used in connection with, the SUBJECT ACCOUNTS (including all current and past trusted or authorized iOS devices and computers, and any devices used to access Apple services), including serial numbers, Unique Device Identifiers ("UDID"), Advertising Identifiers ("IDFA"), Global Unique Identifiers ("GUID"), Media Access Control ("MAC") addresses, Integrated Circuit Card ID numbers ("ICCID"), Electronic Serial Numbers ("ESN"), Mobile Electronic Identity Numbers ("MEIN"), Mobile Equipment Identifiers ("MEID"), Mobile Identification Numbers ("MIN"),

Subscriber Identity Modules ("SIM", Mobile Subscriber Integrated Services Digital Network Numbers ("MSISDN", International Mobile Subscriber Identities ("IMSI", and International Mobile Station Equipment Identities ("IMEI");

c. The contents of all emails associated with the SUBJECT ACCOUNTS, including stored or preserved copies of emails sent to and from the account (including all draft emails and deleted emails, the source and destination addresses associated with each email, the date and time at which each email was sent, the size and length of each email, and the true and accurate header information including the actual IP addresses of the sender and the recipient of the emails, and all attachments;

d. The contents of all instant messages associated with the SUBJECT ACCOUNTS, including stored or preserved copies of instant messages (including iMessages, SMS messages, and MMS messages sent to and from the account (including all draft and deleted messages, the source and destination account or phone number associated with each instant message, the date and time at which each instant message was sent, the size and length of each instant message, the actual IP addresses of the sender and the recipient of each instant message, and the media, if any, attached to each instant message;

e. Any and all WhatsApp messages stored in each account or identifier listed on Attachment A;

f. The contents of all files and other records stored on iCloud, including all iOS device backups, all Apple and third-party app data, all files and other records related to iCloud Mail, iCloud Photo Sharing, My Photo Stream, iCloud Photo Library, iCloud Drive, iWork (including Pages, Numbers, Keynote, and Notes, iCloud Tabs and bookmarks, and iCloud

Keychain, and all address books, contact and buddy lists, notes, reminders, calendar entries, images, videos, voicemails, device settings, and bookmarks;

g. All activity, connection, and transactional logs for the SUBJECT ACCOUNTS (with associated IP addresses including source port numbers), including FaceTime call invitation logs, messaging and query logs (including iMessage, SMS, and MMS messages), mail logs, iCloud logs, iTunes Store and App Store logs (including purchases, downloads, and updates of Apple and third-party apps), My Apple ID and iForgot logs, sign-on logs for all Apple services, Game Center logs, Find My iPhone and Find My Friends logs, logs associated with web-based access of Apple services (including all associated identifiers), and logs associated with iOS device purchase, activation, and upgrades;

h. All records and information regarding locations where the accounts or devices associated with the SUBJECT ACCOUNTS were accessed, including all data stored in connection with Location Services, Find My iPhone, Find My Friends, and Apple Maps;

i. All records pertaining to the types of service used;

j. All records pertaining to communications between Apple and any person or persons regarding any SUBJECT ACCOUNT, including contacts with support services and records of actions taken; and

k. All files, keys, or other information necessary to decrypt any data produced in an encrypted form, when available to Apple (including, but not limited to, the keybag.txt and fileinfolist.txt files).

The Provider is hereby ordered to disclose the above information to the government within 14 days of service of this warrant.

II. Information to Be Seized by the Government

All information described above in Section I that constitutes contraband, fruits, evidence and/or instrumentalities of violations of Title 18, United States Code, Sections 1343 (wire fraud), 1344 (bank fraud), 1349 (bank and wire fraud conspiracy) and 1956 (money laundering and money laundering conspiracy) (the "SUBJECT OFFENSES") that have been committed by KENNETH UKHUEBOR, PATIENCE OSAGIE and any co-conspirators between November 1, 2018 and December 4, 2020, including information pertaining to the following matters:

a. Evidence of communications between and among KENNETH UKHUEBOR, PATIENCE OSAGIE, co-conspirators and/or victims of the SUBJECT OFFENSES, as they relate to the SUBJECT OFFENSES;

b. Evidence of records, photographs and images relating to the SUBJECT OFFENSES, including evidence of any proceeds, monetary or otherwise, received by KENNETH UKHUEBOR and/or PATIENCE OSAGIE through the SUBJECT OFFENSES;

c. Evidence indicating how and when the account(s) were accessed or used, to determine the chronological and geographic context of account access, use and events relating to the crimes under investigation and the account subscriber(s);

d. Any records pertaining to the means and source of payment for services (including any credit card or bank account number or digital money transfer account information);

e. Evidence indicating the subscriber's state of mind as it relates to the SUBJECT OFFENSES; and

f. Evidence that may identify any co-conspirators or aiders and abettors, including records that help reveal their whereabouts.